Quantencomputer
Heisenberg statt Intel

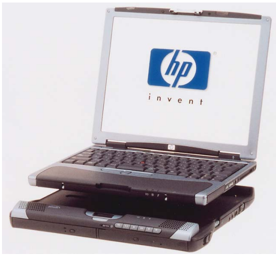
Stephan Mertens

Otto-von-Guericke-Universität, Magdeburg

Computer

ENIAC (1946)

- 19000 Röhren
- 35 Tonnen
- 175 kW
- 300 Mult. pro Sek.

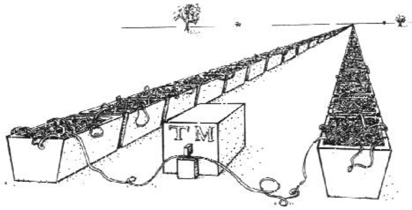


Omnibook 500 (2002)

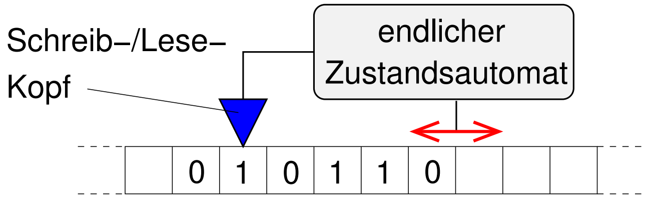
- $> 10^8$ Transistoren
- 1.5 Kg
- < 60 W
- 10^9 Mult. pro Sek.

Turing Maschine

Alan Turing
1912–1954



© Roger Penrose „Computerdenken"

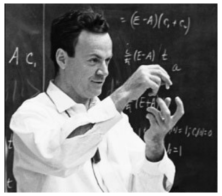


Church-Turing These

> Jeder algorithmische Prozeß läßt sich effizient auf einer Turing-Maschine ausführen.

effizient: n Rechenschritte im Prozeß
$\Rightarrow \mathrm{poly}(n)$ Rechenschritte auf TM

Feynman's Vision



„Klassische Computer können quantenmechanische Systeme prinzipiell nicht effizient simulieren.“ Int.J.Theor.Phys. **21** 467 (1982)

Grund: Hilbert-Raum zu groß!

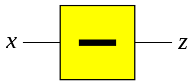
n Spin-$\frac{1}{2}$ Teilchen: $\dim H = 2^n$

Feynman: „Wir sollten Quantencomputer bauen.“

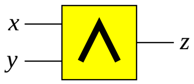
Klassische Computer

Informationseinheit: Das bit

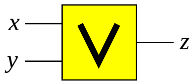
- Formal: $0, 1$
- Physik: Spannung 0 V, 5 V
- Dynamik: Logikgatter



x	z
0	1
1	0



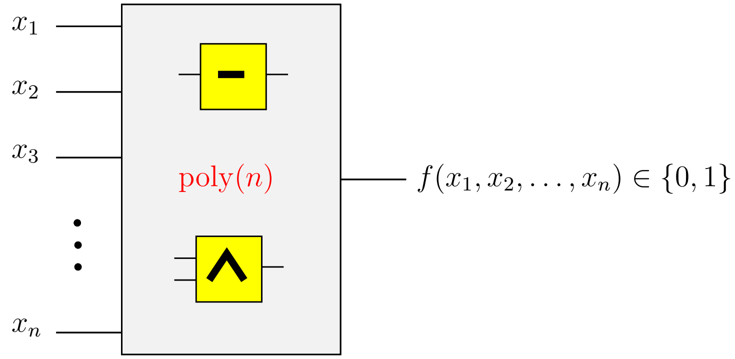
x	y	z
0	0	0
0	1	0
1	0	0
1	1	1



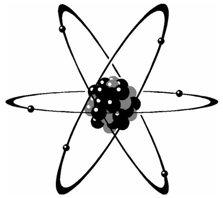
x	y	z
0	0	0
0	1	1
1	0	1
1	1	1

Universalität

Wieviele Gatter(typen) braucht man? Wenige!



Quanten-Bits



Informationseinheit: Das qubit

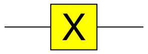
- Formal: $|0\rangle$, $|1\rangle$
- Physik: 2-Zustandssystem
- Dynamik: Unitäre Transformationen

Besonderheiten:

- Überlagerung: $|\Psi\rangle = \alpha_1|0\rangle + \alpha_2|1\rangle$ $\quad |\alpha_1|^2 + |\alpha_2|^2 = 1$
- Register mit n qubits: 2^n Amplituden $\alpha_1, \ldots, \alpha_{2^n}$
- Quanteninformation $\gg$ meßbare Information

1-qubit-Gatter

NOT:

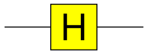


$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

HADAMARD:



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

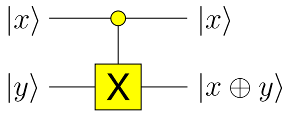
2-qubit-Gatter

controlled NOT (cNOT):

$|00\rangle \mapsto |00\rangle \qquad |01\rangle \mapsto |01\rangle$

$|10\rangle \mapsto |11\rangle \qquad |11\rangle \mapsto |10\rangle$

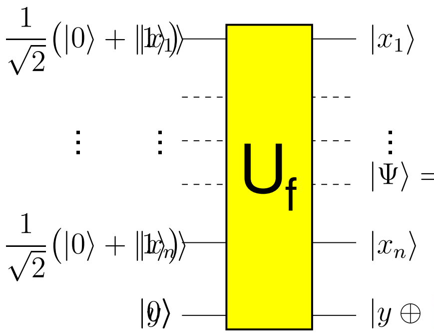
$$U_{\mathrm{CN}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



cNOT $\cup$ 1-qubit-Gatter = universell

Quantenparallelität

$f(x) : \{0,1\}^n \mapsto \{0,1\}$

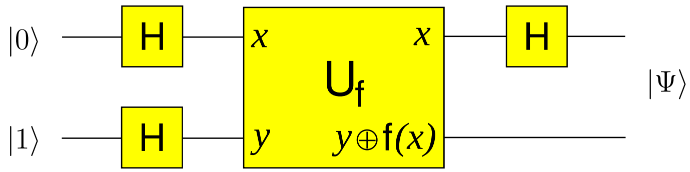


$$|\Psi\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$$

! 2^n Berechnungen in $\mathcal{O}(n)$ Schritten

Deutsch-Josza Transformation

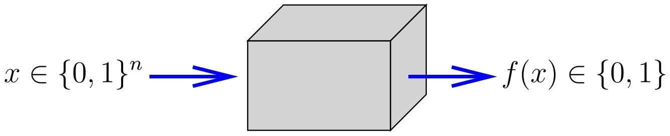
$f(x) : \{0,1\} \mapsto \{0,1\}$



$$|\Psi\rangle = \pm |f(0) \oplus f(1)\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Messung 1. qubit: $\begin{cases} |0\rangle & \text{falls } f(0) = f(1) \\ |1\rangle & \text{falls } f(0) \neq f(1) \end{cases}$

Das Blackbox-Problem



Ist f konstant oder ausgewogen?

- Klassisch: $2^{n-1}+1$ Aufrufe von $f(x)$
- Quantenmechanisch: 1 Aufruf von $f(x)$
- Randomisiert: Fehler $\leq 2^{-k}$ mit $k+1$ Aufrufen von $f(x)$

Starke Church-Turing These

> Jeder algorithmische Prozeß läßt sich
>
> effizient auf einer probabilistischen
>
> Turing-Maschine ausführen.

probabilistisch: TM kann randomisierte Entscheidungen treffen

Ergebnis fehlerbehaftet mit garantierter, vorgebbarer Schranke

Faktorisierung

Gegeben $N \in \mathbb{N}$. Finde $p, q \in \mathbb{N}$ mit $1 < p, q < N$ so daß

$$N = p \times q$$

$$1146833328293 = 1299709 \times 882377$$

- Naiver Ansatz: $\mathcal{O}(\sqrt{N}) = \mathcal{O}(\exp(\frac{1}{2}\log N))$
- Bester klassischer Algorithmus:
$$\mathcal{O}(\exp\left[(\log N)^{1/3}(\log\log N)^{2/3}\right])$$
- Faktorisierung einer 500 stelligen Zahl?
Dauert länger als das Alter des Universums!

N = 15

Euklid: $\mathrm{ggT}(a, N)$ in $\mathrm{poly}(\log N)$ Rechenschritten.

- Wähle Zufallszahl $a < N$, z.B. $a = 6$.
- $\mathrm{ggT}(6, 15) = 3$: Teiler von 15! Glück gehabt!
- Jetzt $a = 7$, $\mathrm{ggT}(7, 15) = 1$.
- Euler: $\exists r \in \mathbb{N}$ mit $a^r \equiv 1 \mod N$
- Hier: $7^4 \equiv 1 \bmod 15$
- $7^4 - 1 = (7^2-1)(7^2+1)$
- $\mathrm{ggT}(7^2-1, 15) = 3$ und $\mathrm{ggT}(7^2+1, 15) = 5$. Fertig!

Faktorisierungs-Algorithmus

Eingabe: $N \in \mathbb{N}$
Ausgabe: Teiler von N oder stop.

- Wähle $a \in \mathbb{N}$ zufällig, $1 < a < N$.
- $\mathrm{ggT}(a, N) > 1$? Ja: Teiler gefunden!
- Finde $r \in \mathbb{N}$ mit $a^r \equiv 1 \bmod N$. !
- Ist r ungerade? stop.
- $(a^{r/2} - 1)$ oder $(a^{r/2} + 1)$ Vielfaches von N? stop
- $\mathrm{ggT}(a^{r/2} \pm 1, N)$ liefert Teiler von N!

$N \neq$ Primzahl: stop mit Wahrsch. $\leq \frac{1}{2}$.

Quantenfaktorisierung

Problem: Gegeben a, N mit $\mathrm{ggT}(a, N) = 1$. Finde r mit

$$a^r \equiv 1 \bmod N$$

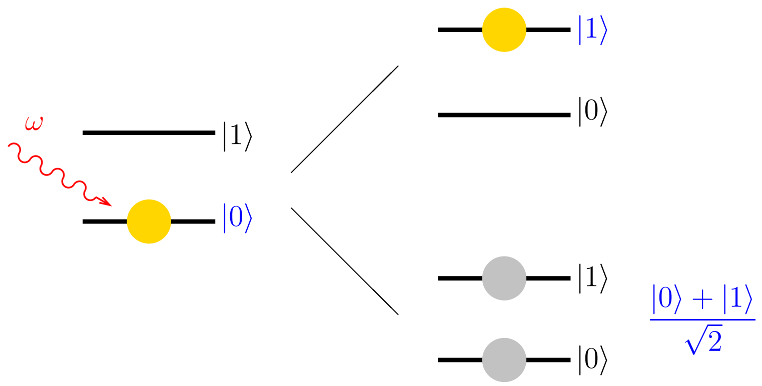
- Betrachten $f : \{1, \ldots, N\} \mapsto \{1, \ldots, N\}$

$$f(x) = (a^x \bmod N)$$

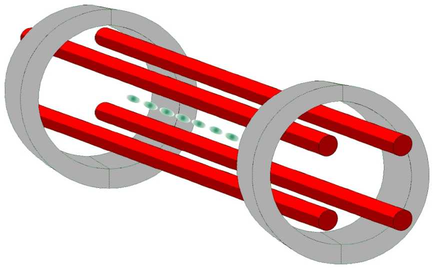
- $f(x + r) = f(x)$: r ist Periode von f.
- Klassisch: FFT in $\mathcal{O}(N \log N)$ Schritten
- Shor (1994): Quanten FFT in $\mathcal{O}(\log^2 N)$ Schritten

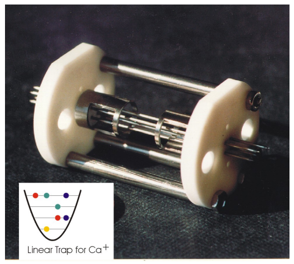
Faktorisierung in $\mathrm{poly}(\log N)$ Schritten auf Quantencomputer!

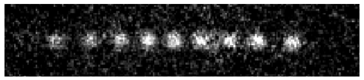
Physikalische qubits



Lineare Ionenfalle





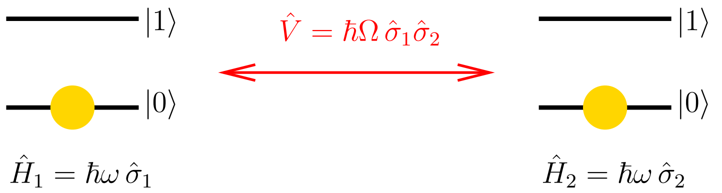


9 eingesperrte Ca^+ Ionen

- RF: 16 MHz, 1000 V
- statisch: 4000 V
- Ionenabst.: ca. 5 μm

Abb.: Institut für Experimentalphysik, Univ. Innsbruck

Physikalische Quantengatter



Resonanz $\omega \pm \Omega$ hängt ab vom Zustand des anderen qubits!

Laserpuls mit $\omega + \Omega$ auf 1. qubit:

$|0\rangle_1 \mapsto |1\rangle_1$ nur, wenn $|x\rangle_2 = |1\rangle$. cNOT !

Rückblick

Quantencomputer

- sind prinzipiell realisierbar (NMR, Spintransport, . . .)
- knacken die besten Verschlüsselungsverfahren
- widerlegen die Church-Turing These—oder nicht?

Und sonst?

- Quantenalgorithmen
- Quantenkryptographie
- Quanteninformationsverarbeitung

Ausblick

Computers in the future may weigh no more than 1.5 tons.

Popular Mechanics, 1949